Data Security

(Elective course-3)

EEC4126

Lecture No. (1)

Dr/ Roayat Ismail Abdelfatah

Course Aims

The aims of this course are to:

- Understand cryptography system
- Classify the encryption algorithms.
- Know the difference between symmetric and asymmetric encryption
- Understand the concepts of data integrity, confidentiality and authentication.
- Study how to apply the security concepts in computer networks.

Student Assessment

Assessment Method	Assessment Length	Schedule	Proportion
Written Examination	3h	On week 16	70%
Oral Assessment	-	-	-
Practical Examination	-	-	-
Semester work	5 hours (overall)	On week 5,9,12	30%

Course Contents

Week	Topics
1,2	Introduction to Cryptography Concepts and mathematics.
3,4,5	Symmetric Key Encryption (Traditional and Modern Techniques)
6,7,8	Asymmetric Key Encryption
10,11,12	Integrity (Hashing), Authentication, and Key Management
13,14	Network Security (IPSec, SSL/TLS, and PGP protocols…etc).

Essential Books:

1. "Information Security, Principles and Practice", Mark Stamp,2005.
2. "Cryptography and Network Security", 4th Edition, Behrouz A. Forouzan,2007.

Web sites:

1. **http://www.tutorialspoint.com/data_communication_computer_network/**
2. **http://learnthat.com/introduction-to-network-security**
3. **WilliamStalling.com/computer Security**
4. **www.pearsoninternational-editions.com/stalling**
5. **ComputerScienceStudent.com**

Introduction to Cryptography Concepts and Mathematics

What is the difference between: "Safety" and "Security"?

- Safety: Deals with the protection of life and assets against fire, natural disasters, and accidents
- Security: Addresses vandalism, theft, and attacks by individuals.

What are the types of security?

1. Physical security: protect people, physical assets and the workplace from various attacks.

But for information we have:

2. Computer Security- COMPUSEC:

Protection of information processed and stored in the computer.

Types of security (cont.)

3. Network security: protection of information in networking devices and connections.
4. Communication security **COMSEC:** protection of information in communication media.

It is the prevention of unauthorized access to telecommunications or information that is transmitted or transferred.

5. Information security INFOSEC:

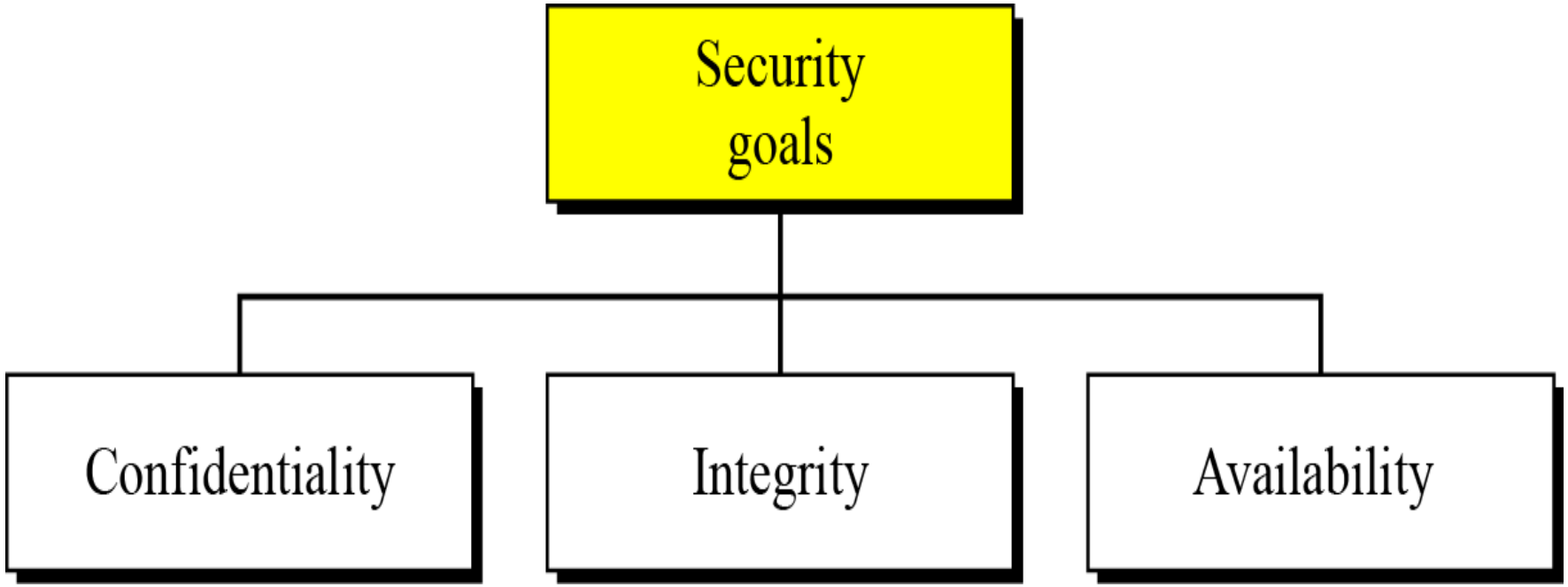
protection of information in all the systems that use , store and transmit it. So it includes all other types of security.

Aspects of Information Security

- We will consider 3 aspects of information security:
  - Security Services (Goals)
  - Security Attacks
  - Security Mechanisms (controls)

Security (Services) Goals

We will first discuss three basic security goals: ***Confidentiality***, ***Integrity*** and **availability**.



Security services for message :

1. Confidentiality (privacy or secrecy)
2. Integrity
3. Availability
4. Authentication
5. Authorization
6. Non-repudiation

1-Confidentiality

Confidentiality, keeping information secret from unauthorized access, is probably the most common goal of information security.

When unauthorized individuals or systems can view information, confidentiality is breached (disclosure).

2- INTEGRITY :

The receiver of message should be able to check whether the message was modified during transmission or not

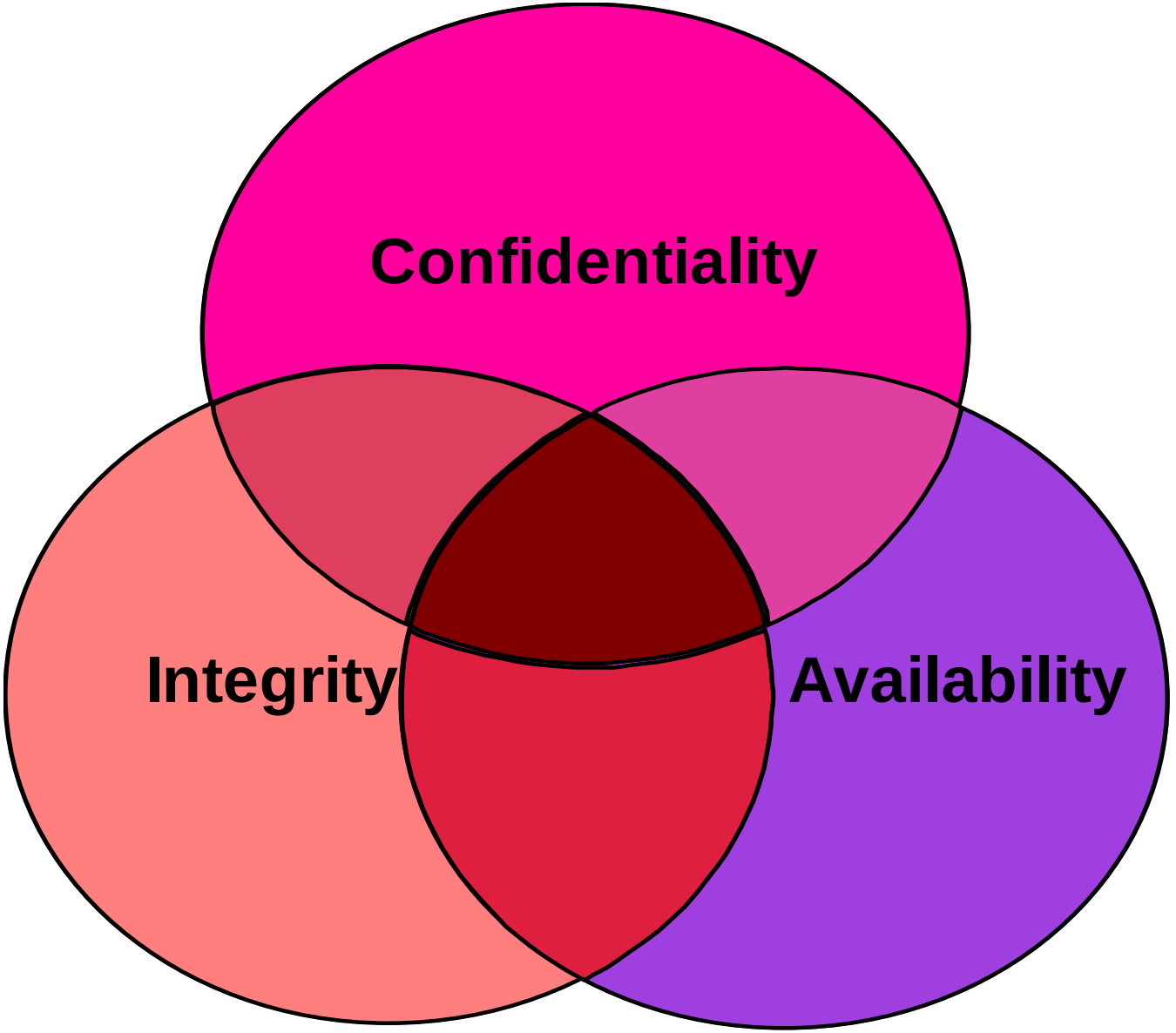
Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of their account needs to be changed. Integrity means that changes should be done only by authorized users and through authorized mechanisms.

- Integrity: is the quality of state of being whole, complete and uncorrupted.
- It is lost due to corruption, damage, destruction during (entering- storing -transmitting)
- Computer viruses and worms are designed to corrupt data.

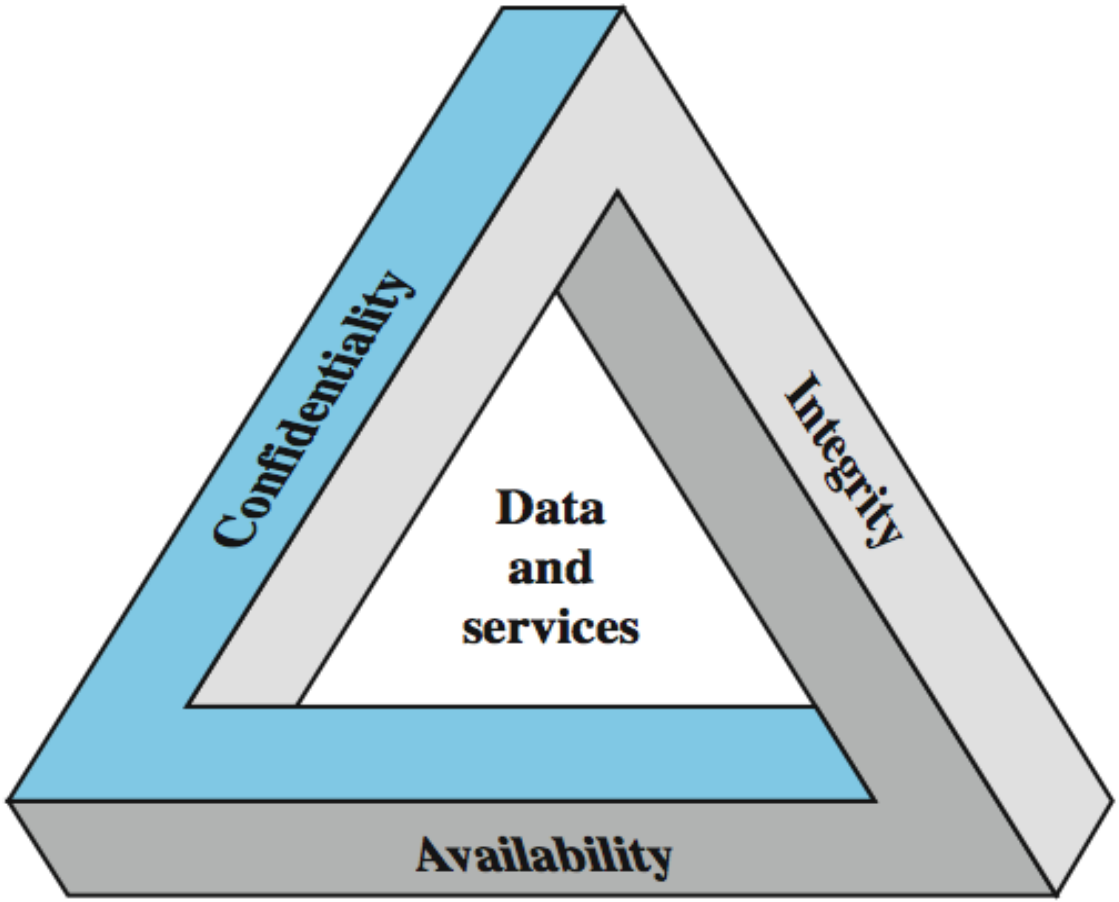
3-Availability

The third component of information security is availability. The information created and stored by an organization needs to be available to authorized users and applications. Information is useless if it is not available. Information needs to be changed constantly, which means that it must be accessible to those authorized to access it.

Unavailability of information is just as harmful to an organization as a lack of confidentiality or integrity. Imagine what would happen to a bank if the customers could not access their accounts for transactions.


Confidentiality
Integrity
Availability

Key Security Concepts



CIA-based Model

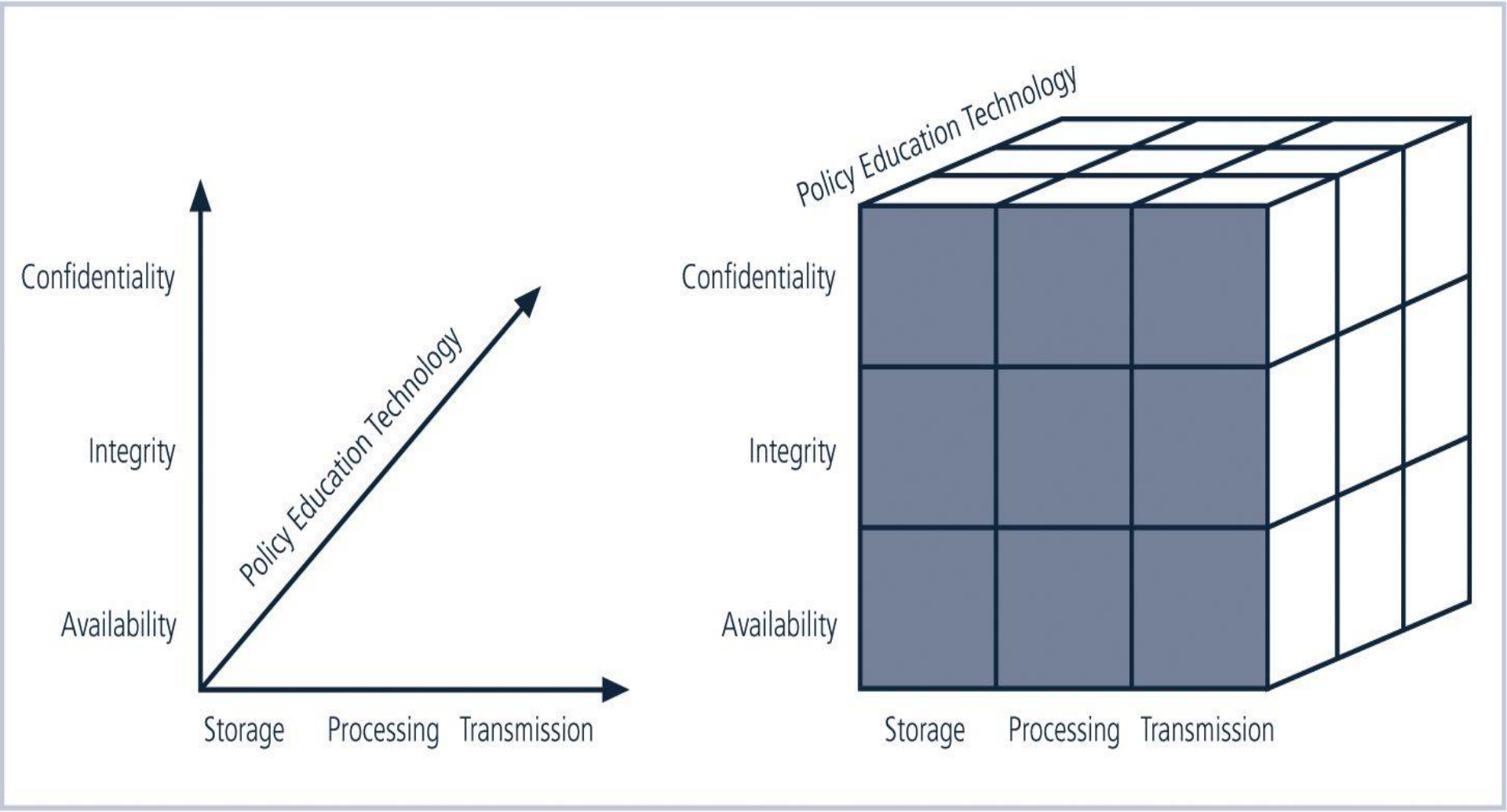


FIG NSTISSC 4011 Security Model (CNSS 4011)

- This model shows the three dimensions centrals of information security.
- 3*3*3 cube with 27 cells. Each cell represents an area of intersection among these three dimensions that must be addressed to secure information systems.
- This model is used to design or review any information security system program.
- You must make sure that each of the 27 cells is properly addressed by each of the three communities of interest.

4. AUTHENTICATION :

The receiver should be sure and verifies the origin of the sender identity , date of message , content

5- NON-REPUDIATION :

Means that the sender of message must not be able to deny sending message that he in fact sends

Potential threats, risks and breaches

Basic definitions:

- Vulnerability
- Threat
- Attack
- Exploit
- Risk
- Breach

Vulnerability – a weakness in the security system that could be exploited to cause harm or loss.

Threat – A possible danger that might exploit a vulnerability to breach security and thus cause possible harm.

EX.: Wall holding back water

- Threat to get wet
- Vulnerability is a crack in the wall

- ***A threat is blocked by control of vulnerability***

An attack:

It is an act or event that exploit a vulnerability.

- An attack is accomplished by a threat agent-

- Attacker must have three things:
  - Method – the skill, knowledge and tool
  - Opportunity – the time and access
  - Motive – a reason to want to perform an attack

An exploit:

- It is a technique or mechanism used to compromise an information assets.
- Vulnerability is also known as the attack surface.
- Vulnerabilities and threats together result in risks to the organization.

Risk

- It is the result of attack.
- It is the possibility of harm
- Harm means: data lost or stolen, or is disclosed or otherwise exposed to unauthorized people for unauthorized purposes. which is an undesirable outcome).
- Breach:

It is a successful attack: occurrence of harm.

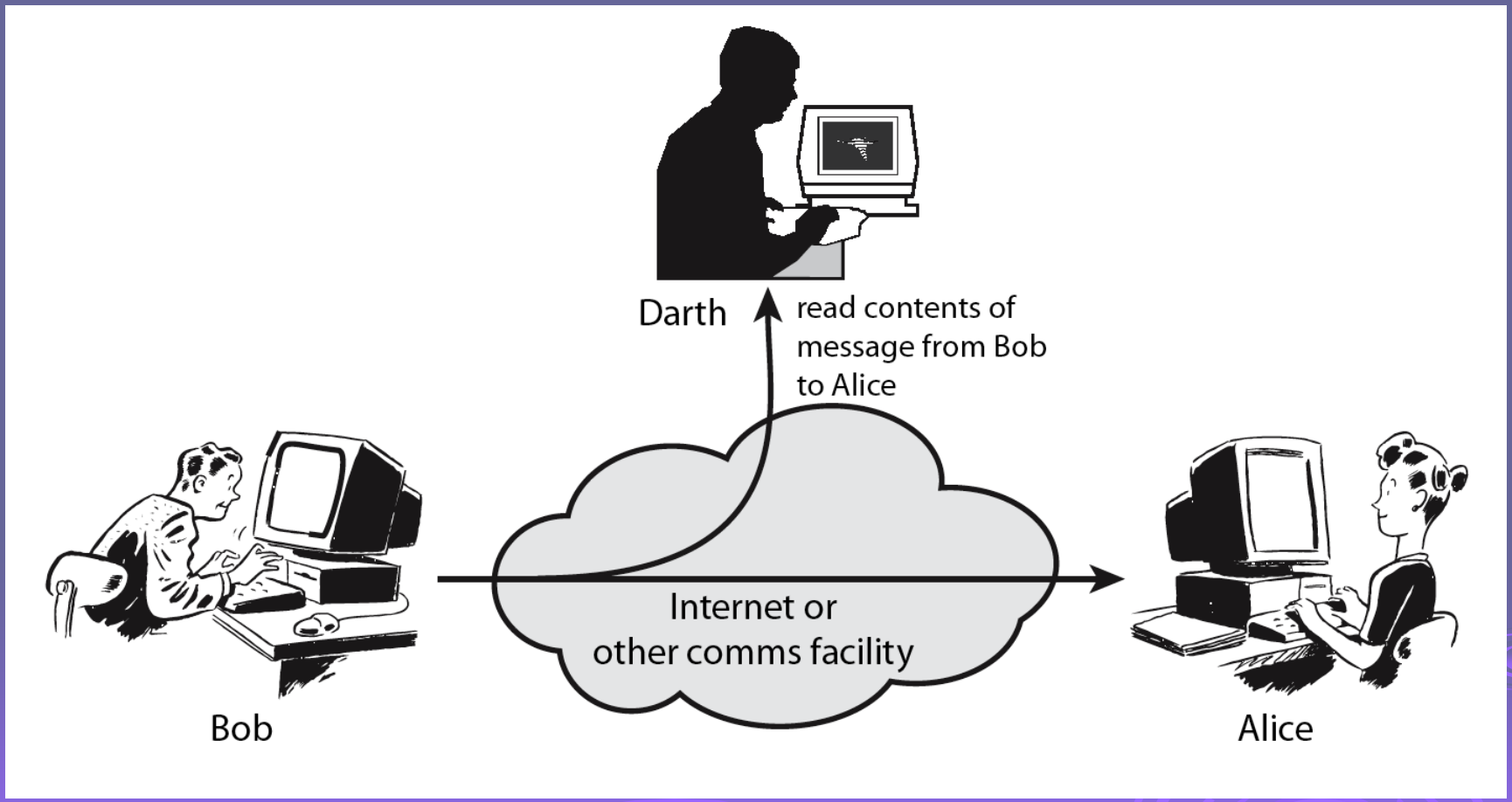
Types of attacks

- Passive attacks
- Active attacks

- A passive attack attempts to learn or make use of information from the system but does not affect system resources.

- *Passive attacks* are in the nature of eavesdropping on, or monitoring of, transmissions.
- The goal of the opponent is to obtain transmitted information.

Passive Attack - Interception



INTERCEPTION :

- defines as unauthorized party gains access to an asset (part of system)

- Attack on confidentiality.

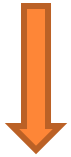
Example :

- Unauthorized copying of files or program

Passive Attack :

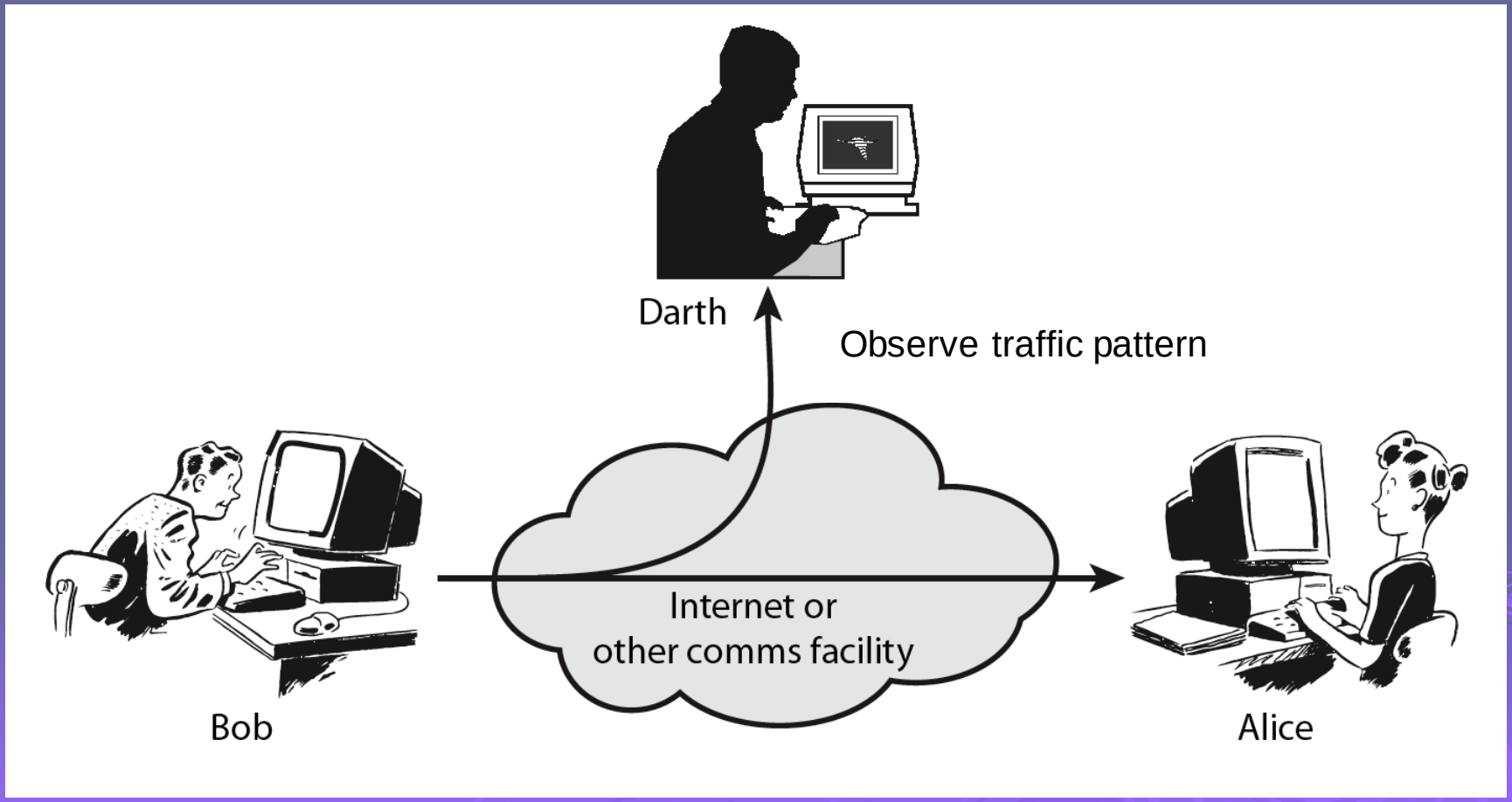
A- Release the message content

B- Traffic Analysis



- Determine the location and identity of communicating parties
- Observe freq and length of cipher text

Passive Attack: Traffic Analysis

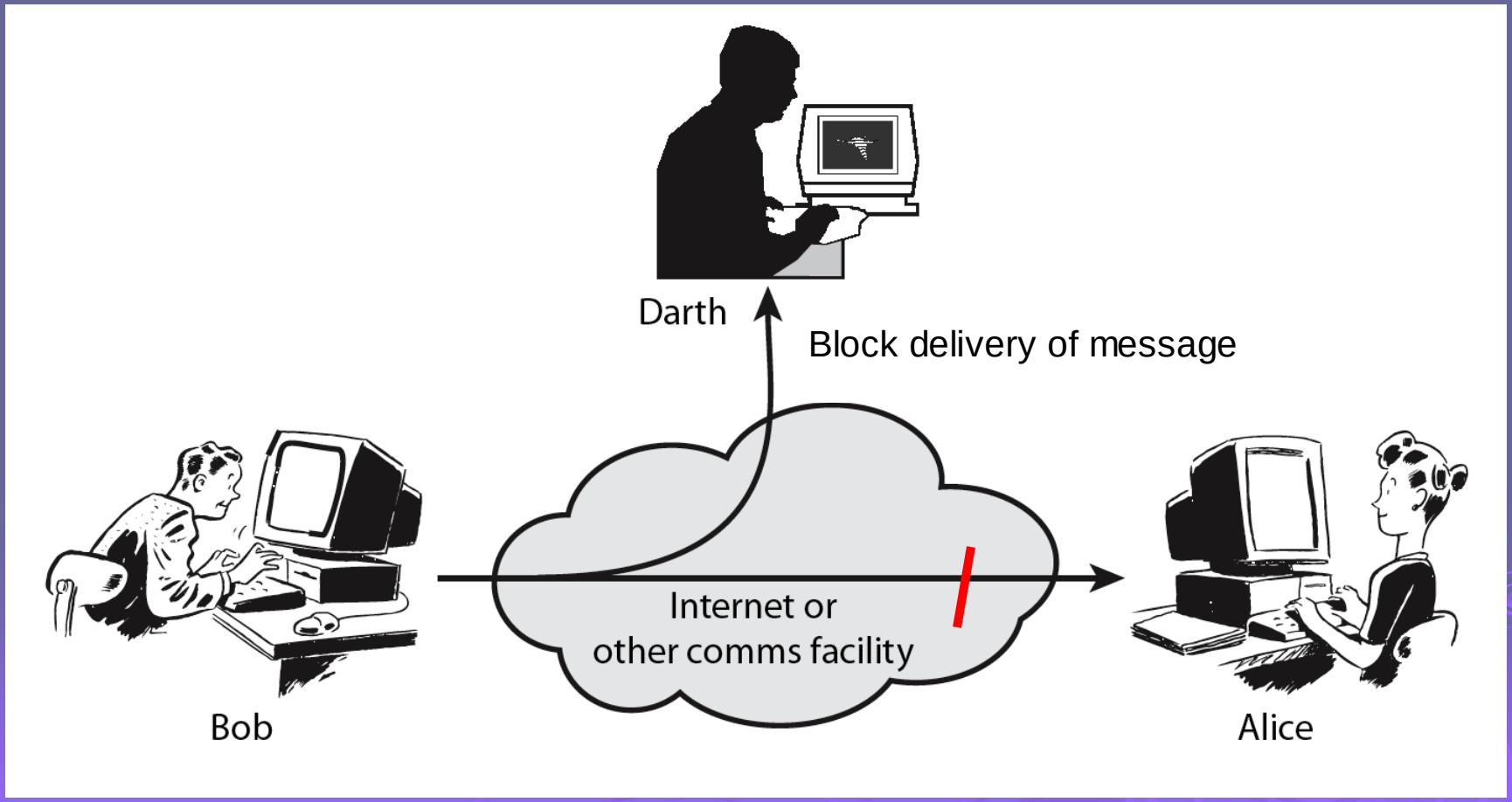


ACTIVE ATTACK

- It involves some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

- Interruption (Denial of service)
- Modification
- Fabrication (Masquerade)
- Replay

Active Attack: Interruption



INTERRUPTION: DENIAL OF SERVICE

- It defines as an asset of the system is destroyed or become unusable.

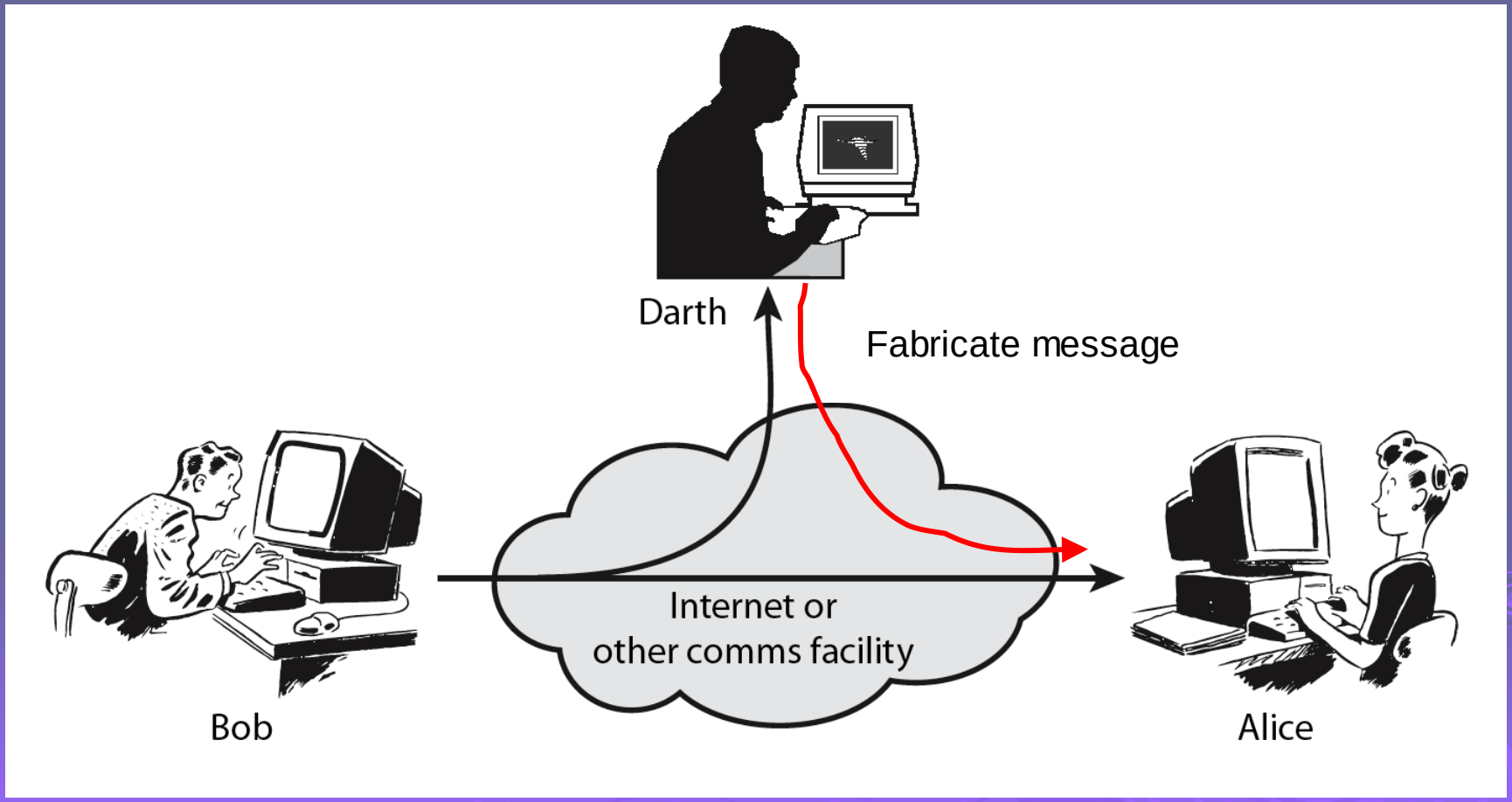
- Attack on availability.
- Denial of service - prevents or inhibits the normal use or management of communications facilities.

Examples :

- An asset (part) of system is destroyed

- Cutting of communication line

Active Attack: Fabrication



Fabrication (Masquerade)

- Defines as unauthorized party inserts counterfeit objectives into system.
- An entity pretends to be a different entity.

- Attack on authentication.
- Insertion of spurious messages in a network.

MODIFICATION

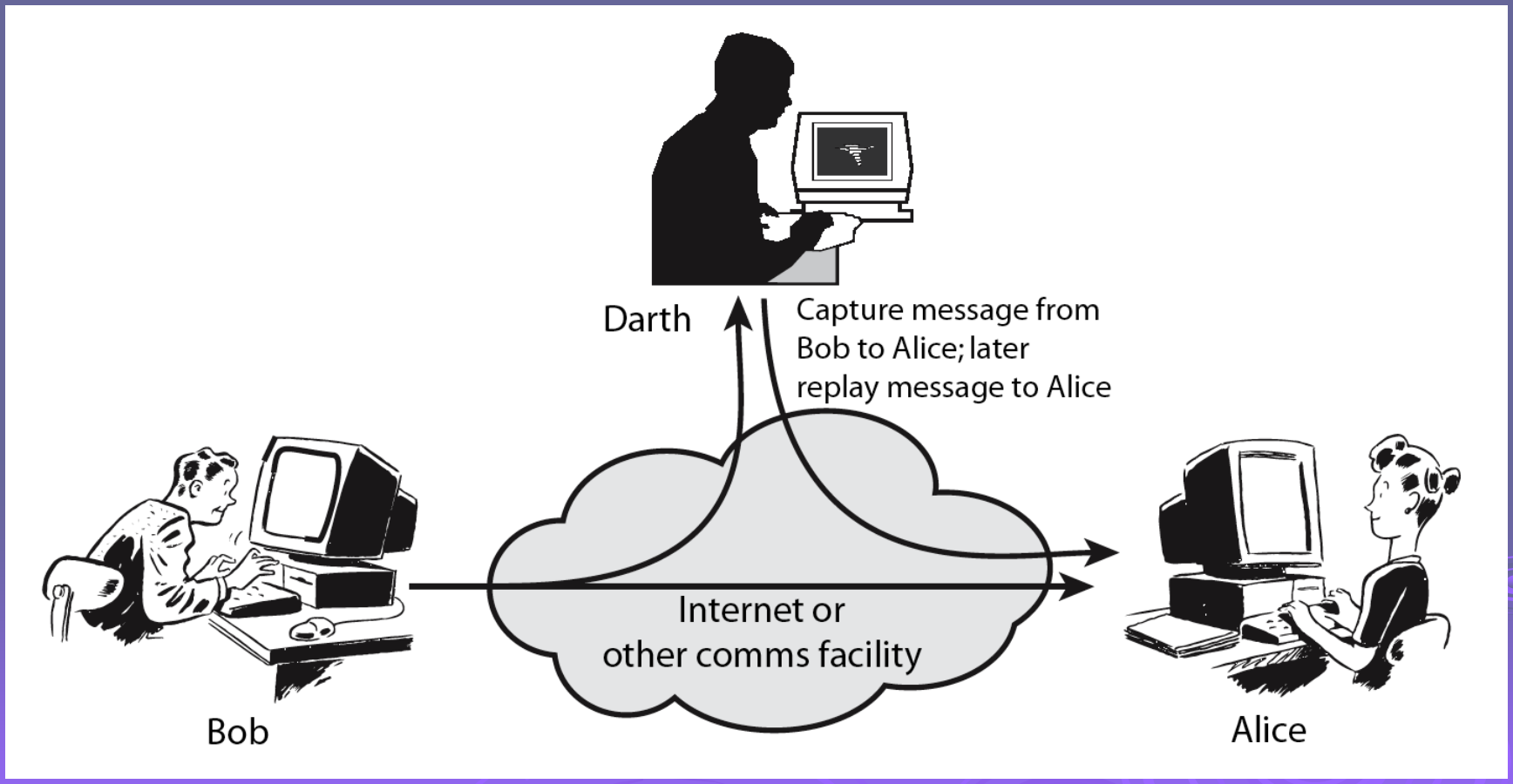
- Modifying the content of message being transmitted in a network which means that an unauthorized party not only gains access but also modify the content of message

- Attack on integrity.

Examples :

- Changing values in data files.

Active Attack: Replay



Replay

- Passive capture of data unit and is subsequent retransmitted to produce an unauthorized effect.

Handling Attacks

- Passive attacks – focus on Prevention
  - Easy to stop
  - Hard to detect
- Active attacks – focus on Detection and Recovery
  - Hard to stop
  - Easy to detect

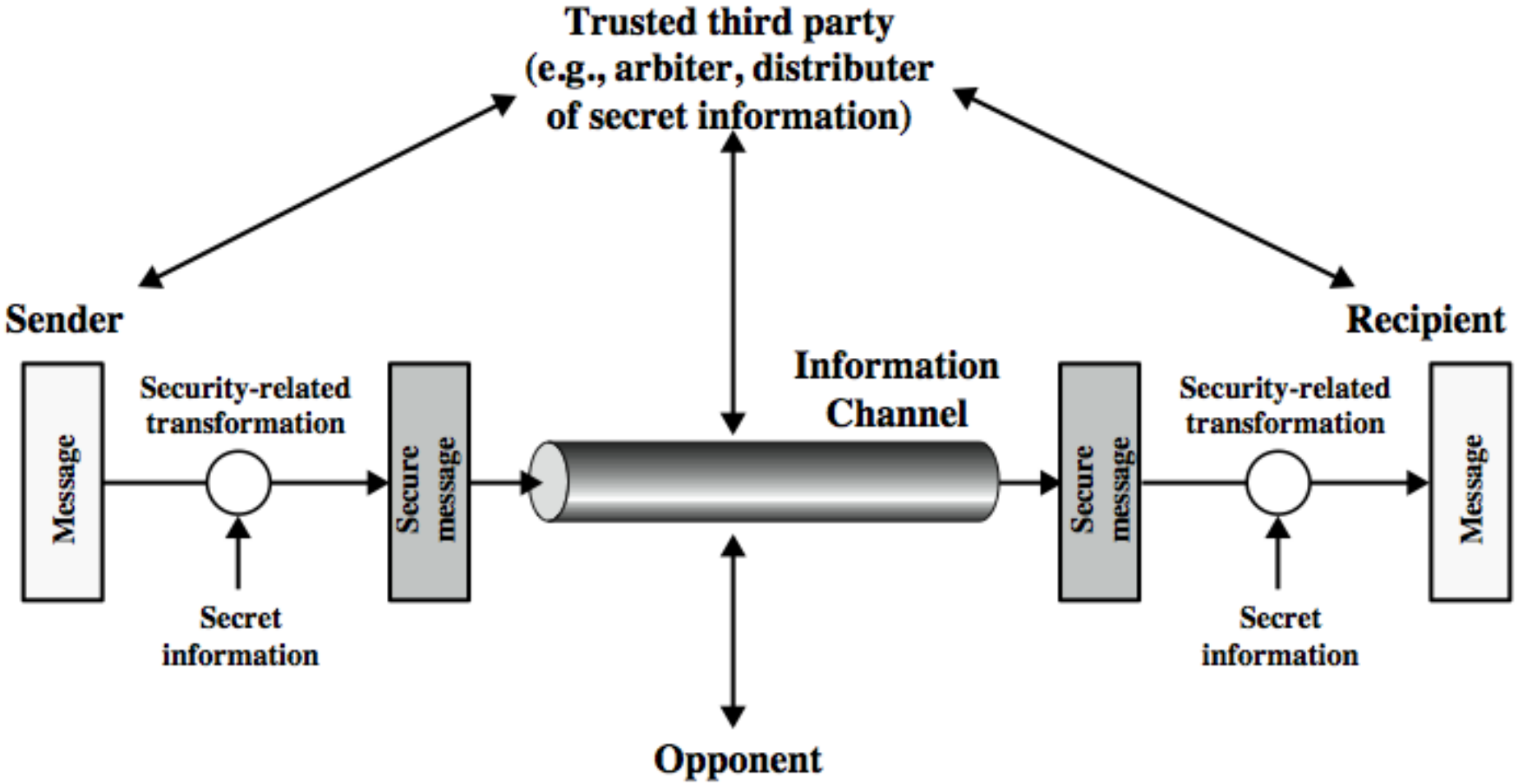
Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required.
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic

Specific security mechanisms:

- Cryptography (encryption ,digital signatures)
- Access controls
- Firewall

Model for Network Security



Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service